

Application No.: 10/702,167
Amendment/Response dated August 20, 2007
Response to Final Rejection dated May 18, 2007

RECEIVED
CENTRAL FAX CENTER

AUG 20 2007

Amendment to the Claims:

This listing of claims will replace all versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A method of secure communication comprising:
establishing a secure tunnel between the at least first and second parties using an encryption algorithm that establishes an encryption key;
authenticating the second party with an authentication server over the secured tunnel establishing an authentication key;
verifying by the first party that the second party possess the same encryption and authentication keys as the first party[[, and]]; and
provisioning secure credentials between the at least first and a network access credential to the second parties using the secured tunnel, responsive to the verifying the second party possess the same encryption and authentication keys as the first party.
2. (Original) The method of claim 1 wherein the communication implementation between the at least first and second parties is at least one of a wired implementation and a wireless implementation.
3. (Original) The method of claim 1 wherein the encryption algorithm is an asymmetric encryption algorithm.
4. (Original) The method of claim 3 wherein the asymmetric encryption algorithm is used to derive a shared secret, subsequently used in the step of establishing a secure tunnel.
5. (Original) The method of claim 3 wherein the asymmetric encryption algorithm is Diffie-Hellman key exchange.

Application No.: 10/702,167
Amendment/Response dated August 20, 2007
Response to Final Rejection dated May 18, 2007

6. (Original) The method of claim 1 wherein the step of authenticating is performed using Microsoft MS-CHAP v2.

7. (Original) The method of claim 1 further comprising a step of provisioning a public/private key pair on one of the at least first and second parties, and then to provision that public key on the respective remaining ones of the at least first and second parties.

8. (Original) The method of claim 7 wherein the step of provisioning a public/private key pair comprises providing a server-side certificate in accordance with Public Key Infrastructure (PKI).

9. (Currently Amended) An implementation for enabling secure communication comprising:

an implementation for establishing a secure tunnel between the at least first and second parties using an encryption algorithm that establishes an encryption key;

an implementation for ~~authentication~~ authenticating the second party with an authentication server using cryptography with an authentication key;

an implementation for verifying by the first party that the second party possess the same encryption and authentication keys as the first party[[, and]]; and

an implementation for providing a network access credential to the second party via the secure tunnel responsive to successfully authenticating the second party and verifying by the first party that the second party possess the same encryption and authentication keys as the first party, ~~for provisioning secure credentials over the secured tunnel between the at least first and second parties.~~

10. (Original) The implementation of claim 9 wherein the implementation for enabling communication between first and second parties is at least one of a wired implementation and a wireless implementation.

11. (Original) The implementation of claim 9 wherein the encryption algorithm is an asymmetric encryption algorithm.

Application No.: 10/702,167
Amendment/Response dated August 20, 2007
Response to Final Rejection dated May 18, 2007

12. (Original) The implementation of claim 11 wherein the asymmetric encryption algorithm is used to derive a shared secret, subsequently used in the step of establishing a secure tunnel.

13. (Original) The implementation of claim 11 wherein the asymmetric encryption algorithm is Diffie-Hellman key exchange.

14. (Original) The implementation of claim 9 wherein the implementation for authenticating comprises Microsoft MS-CHAP v2.

15. (Original) The implementation of claim 9 further comprising an implementation for provisioning a public/private key pair on one of the at least first and second parties, and then to provision that public key on the respective remaining ones of the at least first and second parties.

16. (Original) The implementation of claim 15 wherein the implementation for provisioning a public/private key pair comprises an implementation for providing a server-side certificate in accordance with Public Key Infrastructure (PKI).

17. (Currently Amended) A computer usable medium having computer readable program code embodied in a computer program product comprising:

instructions for communication between at least first and second parties;

instructions for establishing a secure tunnel between the at least first and second parties using an encryption algorithm that establishes an encryption key;

instructions for authenticating between the at least first and second parties over the secured tunnel establishing an authenticating key;

instructions for verifying in the first party that the second party possess the same encryption and authentication keys as the first party[,]; and

instructions for providing a network access credential to the second party via the secure tunnel responsive to the verifying in the first party that the second party possess the same encryption and authentication keys as the first party, for provisioning secure credentials between the at least first and second parties.

Application No.: 10/702,167
Amendment/Response dated August 20, 2007
Response to Final Rejection dated May 18, 2007

18. (Original) The computer program product of claim 17 wherein the instructions for communication between the at least first and second parties comprise instructions for a wireless implementation.

19. (Original) The computer program product of claim 17 wherein the encryption algorithm is a symmetric encryption algorithm.

20. (Original) The computer program product of claim 19 wherein the asymmetric encryption algorithm is used to derive a shared secret, subsequently used in the step of establishing a secure tunnel.

21. (Original) The computer program product of claim 19 wherein the asymmetric encryption algorithm is Diffie-Hellman key exchange.

22. (Original) The computer program product of claim 17 wherein the instructions for authenticating comprise Microsoft MS-CHAP v2.

23. (Original) The computer program product of claim 17 further comprising instructions for provisioning a public/private key pair on one of the at least first and second parties, and then to provision that public key on the respective remaining ones of the at least first and second parties.

24. (Original) The computer program product of claim 17 wherein the instructions for provisioning a public/private key pair comprise instructions for providing a server-side certificate in accordance with Public Key Infrastructure (PKI).

25. (Previously Presented) The method of claim 1, wherein the verifying further comprises hashing the first party encryption key and the authentication key to produce a first hash;

Application No.: 10/702,167
Amendment/Response dated August 20, 2007
Response to Final Rejection dated May 18, 2007

hashing the second party encryption key and the second party authentication key to produce a second hash;

verifying the first and second hash are the same.

26. (Previously Presented) The implementation of claim 9, that further comprises:
an implementation for hashing the first party encryption key and the first party authentication key to produce a first hash;

an implementation for hashing the second party encryption key and the second party authentication key to produce a second hash; and

an implementation for verifying the first and second hash are the same.

27. (Previously Presented) The computer program product of claim 17 further comprising:

instructions for hashing the first party encryption key and the first party authentication key to produce a first hash;

instructions for hashing the second party encryption key and the second party authentication key to produce a second hash; and

wherein the instructions for verifying verify the first hash is the same as the second hash.

28. (New) The method of claim 1, further comprising invalidating a secure credential for the second party responsive to a failure of one of the group consisting of establishing the secure tunnel, authentication, and verifying second party has the same encryption and authentication keys.